

ACG 6415  
Advanced Accounting Information Systems  
Fall 2011

Introduction to IT Security

For the last 22 years the AICPA has conducted a survey in which they solicit responses from “IT Section membership, CITP Credential holders and a selective group of CPAs.” The survey results are intended to shed light on “technology issues that are of greatest importance over the next 12 – 18 months as well as emerging technologies on the horizon” The latest results of this initiative in 2011 ranked as the #1 issue, control and use of mobile devices.

*“The surging use of smartphones and tablets means people are doing business, exchanging sensitive data wherever, whenever they want to,” said Ron Box, CPA/CITP, CFF. “The technology is advancing so rapidly that the capabilities for controlling and protecting the information on mobile devices is lagging behind. What was once as simple as losing your phone, could now create an enormous security risk for organizations.”*

Ranking 2nd in 2011 was Information Security. Thus the two top ranking initiatives identified as being the most important IT initiative for 2011 were security and control related. In fact for the past decade IT security has consistently ranked as the #1 or #2 most important initiative. In 2010 the #1 initiative was:

**Security of data, code & communications / data security & document retention / security threats**

Proper Information Security Management protects the integrity, confidentiality and availability of information in the custody of an organization and reduces the risk of information being compromised.

With two more of the top 10 related to security, #4 and #6 respectively:

**Secure electronic collaboration with clients – client portals**

Portals enable employees, customers, vendors, and other contacts to securely access and share information and documents. Collaboration tools allow multiple users to work together on files of all kinds.

### **Laptop security / encryption**

Stored data can be altered to commit fraud, intercepted by an unscrupulous person en route and altered, and laptops storing vast amounts of confidential information can be lost or stolen.

In 2009 again the #1 initiative was deemed to be Information Security Management. In fact in the report for that year the AICPA indicated that Information Security has been the #1 initiative for the past seven years dating back to the 2003 survey! (It was ranked #3 in 2002 and #1 again in 2001) The #2 and #3 initiatives for 2009 were also security related: Privacy Management and Secure Data File Storage, Transmission and Exchange. Do you see a trend here?

Beginning in 2010 the survey began to also ask AICPA members to rank a list of questions heard most often from audit committees, chief financial officers and chief information officers. I'm guessing you will not be surprised to find that in 2010 the #1 and #2 overheard question were:

- *Are we ensuring that our data and technology resources are protected against hacking, viruses, or other compromises?*
- *Are we considering or implementing organizational security precautions even though we haven't had a data breach or loss?*

In 2011 the top two overheard questions were:

- *Is our information security policy adequate?*
- *Are we ensuring that our data and technology resources are protected against hacking, viruses or other compromises?*

So if IT security, control, IT risk, etc. consistently rise to the top of the IT initiatives list why are accounting programs in general not teaching this to students? Well for one thing it's hard. Also it's not, unless I'm mistaken tested on the CPA exam and hey isn't that what MIS and Computer Science classes are for?

In ACG 6415 we are going to begin to address some of these issues and learn about IT security. We will learn about planning, protecting (an IT word closely associated with the accounting term, control) and responding to IT Security. But first let's take a look at some recent security lapses to frame how important this topic is to individuals, business organizations and sovereign nations.

Let's begin with the sovereign nation part and see how IT security plays a role here. I'm not talking about Wikileaks, in which anarchists obtain classified/private information (legally or illegally) and post it in its raw form for public consumption. Though of course

hacktivism is an increasingly prevalent and important issue with groups like LulzSec and Anonymous playing important roles. For example here in Orlando Anonymous has been identified as a group involved with hacking into Orlando county websites to protest the arrests of individuals feeding the homeless. But no lets talk about how IT security is important for the overall functioning of government projects like delivering electricity, the Internet, transportation infrastructure, etc. And lets talk about one such project, Nuclear facilities.

For more than several years now, Iran has been in the process of enriching Uranium for use in what they say will be power generation. Other's believe that the enriched material will instead be (or at the very least could be) used for making weapons. Although the International Atomic Energy Agency (IAEA) was able to monitor Iran's enrichment they could do nothing to stop it or ensure it was only used for non-combative purposes. Sanctions can be put in place but again are not necessarily always that effective. It was thought until a few years ago that Iran was only a few years away from having enough enriched Uranium to begin producing weapons (that means if they reached this target date they could very possibly have them today). Options were limited to try to stop the program, Israel could bomb and destroy the known enrichment plants but at what cost to the region? The United States likewise could conduct military options but again at what cost? But what if a military strike could be carried out without repercussions? What if the military declared war but it was a cyberwar?

Enter Stuxnet!

*Stuxnet is the name given to a computer worm, or malicious computer program, that began to spread in mid-2009. It may [be] the most sophisticated cyberweapon ever deployed. (NY Times, Stuxnet Page)*

A very brief digression is needed to understand how to produce enriched Uranium (per wikipedia):

*The gas centrifuge process uses a large number of rotating cylinders in series and parallel formations. Each cylinder's rotation creates a strong [centrifugal force](#) so that the heavier gas molecules containing  $^{238}\text{U}$  move toward the outside of the cylinder and the lighter gas molecules rich in  $^{235}\text{U}$  collect closer to the center.*



<http://www.doedigitalarchive.doe.gov/ImageDetailView.cfm?ImageID=1000682&page=search&pageid=thumb>

Stuxnet was able to take over the computers inside some Iranian facilities that controlled the centrifuges. The computers used in Iran were manufactured by Siemens corporation and in 2008 Siemens allowed the United States to test these machines for vulnerabilities. Using either infected e-mail or a USB device the malware was designed to specifically target only the type of Siemens control computers that were involved with the centrifuges. Once these computers were identified, Stuxnet “was programmed to then damage a uranium centrifuge array by repeatedly speeding it up, while at the same time hiding its attack from the control computers by sending false information to displays that monitored the system” (NY Times, Feb 2011). See <https://acg6415.wikispaces.com/Stuxnet> for more. As Ralph Langer pointed out in the video, this type of cyberweapon can be used for any purpose anywhere - we have much to be worried about! Importantly keep in mind the facilities in Iran were NOT connected to the Internet so that alone is not a sufficient control against attacks like this, as we go through the semester think back to this case and why though Access was extremely limited this exploit was still successful.

OK, well most of are probably not going to be working in clandestine uranium enrichment facilities but instead for boring old accounting firms and other business organizations. So let's now turn our attention to a more conventional breach of IT security. What makes this one so interesting is the company that was breached. The company is called HB Gary. On the HBGary (<http://www.hbgary.com/>) website a description is provided of the company, “HBGary, Inc. was founded to provide tools and services to serve the American government and employers who need to protect their assets and information from espionage and international and domestic terrorism. Numerous HBGary principals and employees have proudly served the American military and intelligence agencies and have great pride in the Internet security work that they do to protect American assets and American employers.”

No doubt this company understands security and the importance of security and has been retained by top organizations and governments, thus the story of how HBGary

was hacked is both surprising and troubling for the rest of us mere mortals in trying to protect our companies from attack. Or is it?

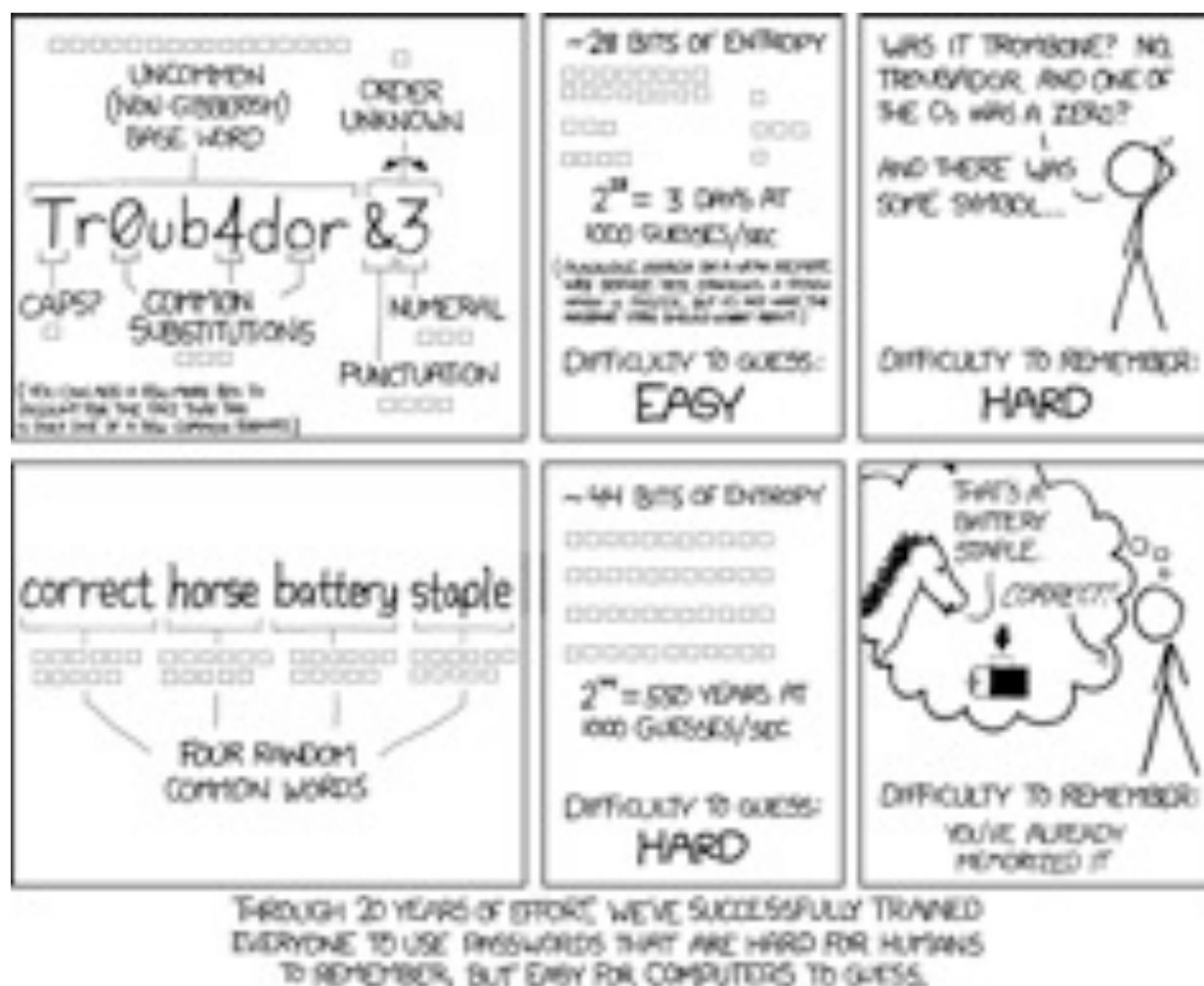
The following summary of an attack that occurred against HBGary while troubling, in fact turns up simple and routine security procedures that any company should and can follow (especially a top IT security firm). As described in an article by Peter Bright of [artstechnica.com](http://artstechnica.com) (2011), “HBGary’s servers were broken into, its e-mails pillaged and published to the world, its data destroyed, and its website defaced. As an added bonus, a second site owned and operated by Greg Hoglund, owner of HBGary, was taken offline and the user registration database published”.

But how could this happen to such a prestigious security firm, well it turns out the security firm wasn’t following its own and most basic of security principles. The initial problem was traced to a piece of custom software that HBGary used for Customer Management (CMS), which was vulnerable to a hack known as a SQL Injection. In short a SQL injection allows a user with access to a web-based form used usually to input data into a system to instead insert code to control the underlying database (deleting it, retrieving information from it, changing data, etc., depending on the code inserted). It is relatively easy to stop SQL injections from occurring by “escaping” (stripping out potential code characters) from data being input into a form before it is inserted or used to query a database – but this wasn’t done in the custom software and bewilderingly wasn’t tested by HBGary (mistake #1). See the figure below for an example of “escaping” in a PHP code:

```
$Nid = mysql_real_escape_string($_POST["id"]);  
$Avatar = mysql_real_escape_string($_POST["AVName"] . "  
Resident");  
$Twitter = mysql_real_escape_string($_POST["TwitterAcct"]);  
$Email = mysql_real_escape_string($_POST["Email"]);
```

This software bug allowed hackers access to the “user database from the CMS — the list of usernames, e-mail addresses, and password hashes for the HBGary employees authorized to make changes to the CMS”. Luckily the passwords weren’t stored in plain text, but were stored as a hash – meaning the hacker would have to break the algorithm to unlock the needed username/password combinations to gain access to the CMS. In the next few weeks will learn what hashing is, how it is done and why some forms of hashing are less secure than others, some might say some types of hashing are actually insecure, or worse giving someone a false sense of security. In the case of HBGary it was found they used one of the weakest hashing algorithms and what’s worse one in which hackers have access to tools that allow them to translate the hashed password into the original password easily and quickly. In the case of the CEO and COO both used passwords that were only 6 digits long and only used lowercase letters (mistake #2).

Had this been the only problem, the hack would have proved embarrassing to HBGary and hackers would have only been able to deface their website. But inexplicably for such a company the poorly constructed and easily hacked passwords were used for multiple systems including e-mail, twitter and LinkedIn (mistake #3) (now you know why even though its a paid you have a pid password, and a nid password, and hopefully multiple passwords for your personal and work log-ins, but see the xkcd cartoon for another opinion) .



Armed with e-mail passwords the hackers were able to send out emails that apparently came from the CEO and thus gained additional security credentials in an unsophisticated phishing attack. This attack is now a non-technical social engineering Phishing exploit (mistake #4):

From: Greg  
 To: Jussi  
 Subject: need to ssh into rootkit

im in europe and need to ssh into the server. can you drop  
open up  
firewall and allow ssh through port 59022 or something  
vague?  
and is our root password still 88j4bb3rw0cky88 or did we  
change to  
88Scr3am3r88 ?  
thanks

---

From: Jussi  
To: Greg  
Subject: Re: need to ssh into rootkit  
hi, do you have public ip? or should i just drop fw?  
and it is w0cky - tho no remote root access allowed

---

From: Greg  
To: Jussi  
Subject: Re: need to ssh into rootkit  
no i dont have the public ip with me at the moment because  
im ready  
for a small meeting and im in a rush.  
if anything just reset my password to changeme123 and give  
me public  
ip and ill ssh in and reset my pw.

---

From: Jussi  
To: Greg  
Subject: Re: need to ssh into rootkit  
ok,  
it should now accept from anywhere to 47152 as ssh. i am  
doing  
testing so that it works for sure.  
your password is changeme123

i am online so just shoot me if you need something.

in europe, but not in finland? :-)

\_jussi

---

From: Greg

To: Jussi

Subject: Re: need to ssh into rootkit

if i can squeeze out time maybe we can catch up.. ill be in  
germany  
for a little bit.

anyway I can't ssh into rootkit. you sure the ips still  
65.74.181.141?

thanks

---

From: Jussi

To: Greg

Subject: Re: need to ssh into rootkit  
does it work now?

---

From: Greg

To: Jussi

Subject: Re: need to ssh into rootkit  
yes jussi thanks

did you reset the user greg or?

---

From: Jussi

To: Greg

Subject: Re: need to ssh into rootkit  
nope. your account is named as hoglund

---

From: Greg

To: Jussi

Subject: Re: need to ssh into rootkit

yup im logged in thanks ill email you in a few, im backed  
up

thanks



To summarize the hack/attack, “A Web application with SQL injection flaws and insecure passwords. Passwords that were badly chosen. Passwords that were reused. Servers that allowed password-based authentication. Systems that weren't patched. And an astonishing willingness to hand out credentials over e-mail, even when the person asking for them should have realized something was up.”

The importance of this story is not that hacking and breach of IT security can take place or even that it did so at an IT Security company of the stature of HBGary, what is important is how easy it would have been to prevent. It doesn't require expensive or complicated controls and processes to be put in place, but common sense use of passwords, password-hashing algorithms for storing passwords and basic assessment of software.

Shall we continue?

On August 18th 2011, this article appeared in Technology Review, **Personal Security** *A wearable jamming technology could protect patients with implants from potentially life-threatening attacks.* The article opens with this paragraph:

*Many medical implants, such as insulin pumps and pacemakers, are equipped with wireless radios that let doctors download data about the patient's condition and adjust the behavior of the implant. But these devices are vulnerable to hackers who can eavesdrop on stored data or even reprogram the implant, causing, for example, a pacemaker to shock a heart unnecessarily.*

Luckily the point of the article was to describe a new technology that is designed to jam an unauthorized wireless link being established between the medical device and a remote terminal.

I could spend the rest of our time here together going over other hacks and security breaches. You should already be aware of the many that have taken place recently. A search of the Privacy Rights Clearinghouse database brings up 93 reported breaches due to hacking on business', educational institutions, governments, medical companies and NGOs. Some of which include:

Date	Company	Breach	# Affected
8/17/2011	Bay Area Rapid Transit	A BART Police Officers Association database was hacked. The names, postal addresses and email addresses of officers were posted online. A French national claimed responsibility for the hack and described the BART site as having zero security in place.	250

Date	Company	Breach	# Affected
8/14/2011	Bay Area Rapid Transit	<p>Anonymous has claimed responsibility for a hack of BART's user database. A list with the first and last names, email addresses, passwords, phone numbers, full addresses and other personal information of MyBart.gov users was posted publicly. MyBart.gov users should change their login information for other sites if they used the same login information for MyBart.gov.</p> <p>Anonymous exposed the security holes in BART's database in order to protest BART's temporary suspension of wireless service throughout BART stations. BART had already been criticized for disabling wireless service in an attempt to counter protests over a fatal officer-involved shooting. The MyBart.gov homepage was also defaced.</p>	2,450

Date	Company	Breach	# Affected
7/8/2011	Capital Grille	<p>A man hacked into the websites of multiple businesses; one of them was the Capital Grill website. He was able to obtain email addresses and passwords of registered customers. A total of 250 people from across the businesses had their information stolen. He then tried to use the login information on financial websites. He was able to access the financial accounts of people who used the same email and password combination. A federal judge sentenced him to 10 years in prison.</p>	250
7/18/2011	<b>Beth Israel Deaconess Medical Center</b> <b>Boston, Massachusetts</b>	<p>A vendor failed to restore computer security controls following routine maintenance. A virus was later discovered on a computer that contained names, medical record numbers, genders, dates of birth, and the date and name of radiology procedures for patients. The virus transmitted encrypted data files to an unknown location. The computer was cleaned and had its software re-installed to clear the virus.</p>	2,012

Date	Company	Breach	# Affected
6/26/2011	PBS	<p>Hackers managed to obtain a number of administrative usernames and passwords for the PBS website. PBS became aware of the intrusion when a phony news story was placed on the website in late May. The login information for over 200 database users was later posted on the internet.</p> <p>Hackers then began releasing additional information on the PBS website and member database. The names, addresses, email addresses of subscribers. The hackers claim that they may release phone numbers and passwords of PBS members as well. Wyoming PBS was also breached.</p>	69,000

Date	Company	Breach	# Affected
6/19/2011	<b>SEGA</b>	<p>The SEGA Pass website was hit by hackers sometime around June 16. Sega Europe in London operates the website, but customers worldwide may have been affected.</p> <p>No credit card information was exposed, but names, dates of birth, email addresses and encrypted passwords were stolen by the hackers. Sega recommends that customers change login information for other sites if they used the same login information for SEGA Pass. Sega reported that 1,290,755 customers were affected.</p>	1,290,755
6/9/2011	<b>Citibank</b>	<p>Hackers have managed to access the information of approximately 1% of Citibank's 21 million users. U.S. Customer names, account numbers, and contact information were exposed. Security codes and dates of birth were not exposed. The breach occurred sometime in May.</p>	360,000 reported - most likely higher

Date	Company	Breach	# Affected
4/27/2011	SONY Playstation	Sony discovered [6] an external intrusion on PSN and its Qriocity music service around April 19. Sony placed an outage to block users from playing online games or accessing services like Netflix and Hulu Plus on Friday April 22. Sony says the outage will continue until the situation is addressed, which will likely be within the next week. Sony believes an unauthorized person has obtained names, addresses, email addresses, dates of birth, PlayStation Network/Qriocity password and login, and handle/PSN online IDs for multiple users. The attacker may have also stolen users' purchase history, billing address, and password security questions. User credit card numbers may have also been obtained.	101.6 million users 12 million unencrypted credit cards

The point is that hacking and data breaches are becoming more and more prevalent, in fact a daily occurrence almost. When we think about what accounting is - the collection, recording and processing of information to support internal and external decision making - and the fact that if this information is un-reliable than those decisions will also be suspect. If you understand that most organizations largest assets are its data and how vulnerable that data can be you will understand the need to begin an exploration into IT security. As accountants our role among others is to help put in controls to safeguard a companies assets, we can not perform this obligation without understanding IT security. Not to get all "accounting" but you should also understand

that compliance with Sarbanes-Oxley also requires accountants to report on the Internal Control of company systems and this includes there Information Systems and IT Security Management Systems and will discuss this some in the next few weeks.

At times this class might get very technical for some of you, but rest assured the goal of this course is not to make any of you IT Security professionals or hackers for that matter. It is simply to expose you to what the AICPA survey has been pointing out for over a decade, IT security, control, privacy of customer data are and will continue to be extremely high priorities for CPA and the organizations they work for.